David Beydler
MATH 540A
Due: 10/10/07

1.7-17, 18   2.1-11

$\boxed{1.7}$

17) [Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by

$$x \mapsto gxg^{-1}.$$

For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e., is an automorphism of G). Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$).]

Pf: Fix $g \in G$. Let $\phi_g : G \to G$ be defined by $\phi_g(x) = gxg^{-1}$. Then, for $g_1, g_2 \in G$,

$$\begin{aligned}\phi_g(g_1 g_2) &= g g_1 g_2 g^{-1} \\ &= g g_1 1 g_2 g^{-1} \\ &= g g_1 g^{-1} g g_2 g^{-1} \\ &= \phi_g(g_1)\phi_g(g_2)\end{aligned}$$

Thus, ϕ_g is a homomorphism. Now define $\psi_g : G \to G$ by $\psi_g(x) = g^{-1}xg$. Then, for $x \in G$,

$$\psi_g(\phi_g(x)) = \psi_g(gxg^{-1}) = g^{-1}gxg^{-1}g = 1 \cdot x \cdot 1 = x, \text{ and}$$
$$\phi_g(\psi_g(x)) = \phi_g(g^{-1}xg) = gg^{-1}xgg^{-1} = 1 \cdot x \cdot 1 = x$$

Thus, $\psi_g = \phi_g^{-1}$. Since ϕ_g has an inverse and is a homomorphism, it is an isomorphism.

see next page

DB2

(1.7 cont) (17 cont)

Now, let $x \in G$. The order of x is either finite or infinite. Suppose the order is finite. Then $|x| = n$ for some positive integer n. Then

$$\begin{aligned}(gxg^{-1})^n &= \underbrace{(gxg^{-1})(gxg^{-1})\ldots(gxg^{-1})}_{n \text{ times}} \quad \text{Each } g^{-1}g = 1 \\ &= gx \cdot 1 \cdot x \cdot 1 \ldots 1 \cdot xg^{-1} \\ &= g\underbrace{xx\ldots x}_{n \text{ times}}g^{-1} \\ &= gx^n g^{-1} \quad \text{Since } |x| = n,\ x^n = 1. \\ &= g1g^{-1} \\ &= gg^{-1} \\ &= 1\end{aligned}$$

So, $|gxg^{-1}| \leq n$. Suppose $|gxg^{-1}| = m$, where $m < n$. Then we would have

$$\begin{aligned}1 &= (gxg^{-1})^m \quad \text{By an argument similar to the above one.} \\ &= gx^m g^{-1}\end{aligned}$$

So, $x^m = g^{-1} \cdot 1 \cdot g = 1$. But this would contradict the fact that $|x| = n$! So, $|gxg^{-1}| = n$. Therefore, $|x| = |gxg^{-1}|$.

see next page

(1.7 cont) (17 cont)

To show that $|A| = |gAg^{-1}|$ we can make a bijection from A to gAg^{-1} as follows. Define $f: A \to gAg^{-1}$ as $f(a) = gag^{-1}$, and define $h: gAg^{-1} \to A$ as $h(gag^{-1}) = a$. Thus, if $a \in A$, then

$$f(h(gag^{-1})) = f(a) = gag^{-1}, \text{ and}$$
$$h(f(a)) = h(gag^{-1}) = a$$

So, $h = f^{-1}$. Thus, f is a bijection from A to gAg^{-1}, so $|A| = |gAg^{-1}|$. ▨

(1.7 cont) 18) [Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \text{ iff } a = hb \text{ for some } h \in H$$

is an equivalence relation. (For each $x \in A$ the equivalence class of x under $\sim$ is called the orbit of x under the action of H. The orbits under the action of H partition the set A.)]

Pf: To show that $\sim$ is an equivalence relation, we need to show that it is reflexive, symmetric, and transitive.

Reflexive: Let $a \in A$. Since H is a group, $1 \in H$. And since H acts on A, $1 \cdot a = a$. So, $a \sim a$.

Symmetric: Let $a, b \in A$ such that $a \sim b$. So, $a = hb$ for some $h \in H$. Then, $h^{-1}a = h^{-1}(hb)$. Since H acts on A, $h^{-1}(hb) = (h^{-1}h)b = 1 \cdot b = b$. So, $h^{-1}a = b$. Since $h^{-1} \in H$, we conclude that $b \sim a$.

Transitive: Let $a, b, c \in A$. Suppose $a \sim b$ and $b \sim c$. Then $a = h_1 b$ and $b = h_2 c$ for some $h_1, h_2 \in H$. So, $a = h_1(h_2 c)$. Since H acts on A, we have $h_1(h_2 c) = (h_1 h_2)c$. So, $a = (h_1 h_2)c$. Since $h_1 h_2 \in H$, we conclude that $a \sim c$.

Thus, $\sim$ is an equivalence relation. ∎

$\boxed{2.1}$ 11) [Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:]

a) $[\{(a,1) \mid a \in A\}]$

Pf: Let $S = \{(a,1) \mid a \in A\}$. First, since A is a group, $(1,1) \in S$. Now, let $(a_1,1), (a_2,1) \in S$. Then $(a_2^{-1},1) \in S$ since $a_2^{-1} \in A$. So, since

$$(a_2,1)(a_2^{-1},1) = (a_2 a_2^{-1}, 1\cdot 1) = (1,1), \text{ and}$$
$$(a_2^{-1},1)(a_2,1) = (a_2^{-1}a_2, 1\cdot 1) = (1,1),$$

$(a_2^{-1},1) = (a_2,1)^{-1}$. So,

$$(a_1,1)(a_2,1)^{-1} = (a_1,1)(a_2^{-1},1) = (\underbrace{a_1 a_2^{-1}}_{\in A}, 1) \in S$$

Thus, S is a subgroup of $A \times B$. ▨

see next page

(2-1 cont) (11 cont)

b) [$\{(1,b) \mid b \in B\}$]

Pf: Let $S = \{(1,b) \mid b \in B\}$. Since B is a group, $(1,1) \in S$. Now, let $(1,b_1), (1,b_2) \in S$. Then $(1, b_2^{-1}) \in S$ since $b_2^{-1} \in B$. So, since

$$(1,b_2)(1,b_2^{-1}) = (1\cdot 1, b_2 b_2^{-1}) = (1,1), \text{ and}$$
$$(1,b_2^{-1})(1,b_2) = (1\cdot 1, b_2^{-1} b_2) = (1,1),$$

$(1,b_2^{-1}) = (1,b_2)^{-1}$. So,

$$(1,b_1)(1,b_2)^{-1} = (1,b_1)(1,b_2^{-1})$$
$$= (1, \underbrace{b_1 b_2^{-1}}_{\in B}) \in S$$

Thus, S is a subgroup of $A \times B$. $\boxtimes$

c) [$\{(a,a) \mid a \in A\}$, where here we assume $B = A$]

Pf: Let $S = \{(a,a) \mid a \in A\}$. Then $(1,1) \in S$. Now, let $(a_1,a_1), (a_2,a_2) \in S$. Then $(a_2^{-1}, a_2^{-1}) \in S$ since $a_2^{-1} \in A$. So,

$$(a_2,a_2)(a_2^{-1}, a_2^{-1}) = (a_2 a_2^{-1}, a_2 a_2^{-1}) = (1,1), \text{ and}$$
$$(a_2^{-1}, a_2^{-1})(a_2,a_2) = (a_2^{-1} a_2, a_2^{-1} a_2) = (1,1),$$

thus, $(a_2^{-1}, a_2^{-1}) = (a_2,a_2)^{-1}$. So,

$$(a_1,a_1)(a_2,a_2)^{-1} = (a_1,a_1)(a_2^{-1}, a_2^{-1})$$
$$= (\underbrace{a_1 a_2^{-1}}_{\in A}, \underbrace{a_1 a_2^{-1}}_{\in A}) \in S$$

So, S is a subgroup of $A \times B$ ($= A \times A$.) $\boxtimes$